UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/019,344	12/21/2001	Frank Muller	PTT-128 (402571US)	8722

7265 7590 08/18/2005

MICHAELSON AND WALLACE
PARKWAY 109 OFFICE CENTER
328 NEWMAN SPRINGS RD
P O BOX 8489
RED BANK, NJ 07701

EXAMINER	
DERWICH, KRISTIN M	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/019,344	MULLER ET AL.	
	Examiner	Art Unit	
	Kristin Derwich	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *8-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/21/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 8-14 are pending.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 8-14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Any claims that are not explicitly addressed are rejected based upon their dependency.

2. Regarding claim 8, the phrase "such as" in line 6 renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

3. Regarding claim 8, the phrase "and the like" at line 7 renders the claim(s) indefinite because the claim(s) include(s) elements not actually disclosed (those encompassed by "and the like"), thereby rendering the scope of the claim(s) unascertainable. See MPEP § 2173.05(d).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Hereafter patent literature that is referenced as prior art will be cited by column and line number in the form of (column number:line number range). For example, the citation (6:23-27) refers to lines 23-27 of the 6th column in the reference.

4. Claims 8 and 14 rejected under 35 U.S.C. 103(a) as being unpatentable over Moroney et al. (Moroney), U.S. Patent No. 5,054,067 in view of Kocher et al. (Kocher), U.S. Patent No. 6,327,661.

As per claim 8:

Moroney substantially teaches loading plaintext and an encryption key (2:29-35) into both linear and nonlinear feedback shift registers to produce a pseudorandom nonlinear sequence (3:1-12). Moroney fails to teach this method as it would apply to protecting a smart card from attack. However, Kocher discloses a method wherein a pseudorandom number generator is used in clock skipping (7:24-29) in order to protect a smart card from attack (6:19-22).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize Moroney's pseudorandom number generator because it would have increased the randomness of the pseudorandom generator thus increasing the security of the system as a whole (Moroney, 1:46-58).

As per claim 14:

Moroney and Kocher substantially teach a method for protecting a card as applied to claim 8 above and furthermore, Moroney discloses a method wherein the remaining bytes of the N bytes produced by the key are loaded into a strictly linear feedback shift register, hence they are loaded utilizing only a linear feedback function and in order to produce the rest of the key stream, clocking on must occur thereafter (3:5-12).

5. Claims 9, 10 and 13 rejected under 35 U.S.C. 103(a) as being unpatentable over Moroney (U.S. 5,054,067) in view of Kocher (U.S. 6,327,661) as applied to claim 8 above, and further in view of Shimada, U.S. Patent No. 6,278,780.

As per claim 9:

Moroney and Kocher substantially teach a method for protecting a card as applied to claim 8 above and furthermore, Shimada discloses a method wherein after in internal key has been loaded into the shift register, it clocks on and data bits are loaded (2:4-12).

It would have been obvious at the time of applicant's invention to utilize Shimada's internal crypto-key generator in order to produce the initial values in Moroney's pseudorandom number generator in order to prevent a third party from tapping the data sequence without permission (Shimada, 1:6-14).

As per claim 10:

Moroney and Kocher substantially teach a method for protecting a card as applied to claim 8 above and furthermore, Shimada discloses a method wherein

after the shift register has been clocked on, the shift register's contents are filled with bits generated by the initial key since (2:4-12).

As per claim 13:

Moroney and Kocher substantially teach a method for protecting a card as applied to claim 8 above and furthermore, Shimada discloses a method wherein the internal keys generated are utilized as initial keys for linear feedback shift registers (1:6-14). Since they are the initial key, the content of the shift register is fixed in that it is always empty in order for the initial key to be loaded.

6. Claim 11 and 12 rejected under 35 U.S.C. 103(a) as being unpatentable over Moroney in view of Kocher as applied to claim 8 above, and further in view of Rose, U.S. Patent No. 6,510,228.

As per claim 11:

Moroney and Kocher substantially teach a method for protecting a card as applied to claim 8 above and furthermore, Rose discloses a method wherein at certain clock cycles an output in not generated, thus no new data is being loaded into the shift register during or prior to this clocking on period (12:12-25).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to avoid loading data during certain clocking periods to produce stuttering in the stream cipher which would increase the non-linearity of the stream and thus increase the protection against attack (11:60-64).

As per claim 12:

Since the data is not being loaded into the shift register as mentioned in claim 11, the input data is not connected to the shift register since it is not being loaded during the clocking on period.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin Derwich whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kristin Derwich
Examiner

KD

Art Unit 2132

GILBERTO BARRÓN JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100